An assessment of UK insolvency laws in the light of new ways of working in the era of Covid-19

Rebecca Parry, Nottingham Trent University, rebecca.parry@ntu.ac.uk

The Covid-19 pandemic has brought changes to working, including greater reliance on technologies, including cloud computing. This calls for a reassessment of current insolvency laws, given the potential risks of business interruption and loss to consumers arising from the failure of a cloud service provider. While noting the limitations on the ability of domestic insolvency laws to handle these insolvencies, which are supranational in nature, this article assesses the suitability of current insolvency laws in England and Wales to enable the managed closedown of a cloud service provider with minimal loss and disruption to customers.

Background

The Covid-19 pandemic has brought rapid changes to insolvency legislation to many countries, including in the UK,[1] and much attention has focused on how new procedures will affect the dynamics of the economy in their impact on creditors, including suppliers of goods and services and landlords.[2] Attention also needs to be paid, however, to profound changes in professional activities necessitated by the pandemic and the suitability of the expanded suite of UK insolvency procedures for handling insolvencies that may impact on businesses in this changed environment. Boosted by technological advancements, the pandemic has accelerated changes to ways of doing work.[3] Working from home has been done on a far greater scale than in the past, through meetings and other collaborations being done online. In this context attention has rightly been drawn to a need for cybersecurity, data protection and privacy.[4] However it is important also to pay attention to the implications of reliance on cloud computing services, which support many of the new ways of working and dependence on which has already been noted as presenting the significant risks to users.[5] The cloud is used for various activities, including to organise projects, set up virtual desktops for employees, store and process data and access software as well as to outsource functions. One of the attractions of the cloud is as an alternative to storage of data on employees' own

[1] Primarily in the Corporate Governance and Insolvency Act 2020, discussed further below.

[2] For a detailed review of the new UK laws see for example Richard Tett and Katharina Crinson, 'The Most Important Insolvency Reforms for a Generation' (2020) 17 *International Corporate Rescue* 243; Gerard McCormack, INSOL Special Report: Permanent changes to the UK's corporate restructuring and insolvency laws in the wake of Covid-19' (INSOL International, 2020).

[3] This article builds upon Rebecca Parry & Roger Bisson, 'Legal approaches to management of the risk of cloud computing insolvencies' (2020) 20 *Journal of Corporate Law Studies* 421-451, DOI: 10.1080/14735970.2020.1724504. For recognition from the technology sector see e.g. Friedman, Z. 2020. "How COVID-19 Will Change the Future of Work." (*Forbes*, 2020). <www.forbes.com/sites/zackfriedman/2020/05/06/covid-19-future-of-work-coronavirus/#5b1320a273b2> May 6 2020.

[4] See e.g. Luca Rahilly (ed), *McKinsey on Risk* (McKinsey, 2020) < https://www.mckinsey.com/business-functions/risk/our-insights/mckinsey-on-risk/mckinsey-on-risk-special-issue-on-the-covid-19-crisis>.

[5] Lloyd's, 'Cloud Down, Impacts on the US Economy, Emerging Risk Report 2018' (Lloyds, 2018), <www.lloyds.com/news-and-insight/risk-insight/library/technology/cloud-down>, accessed 3 September 2020 'reliance on a relatively small number of companies has resulted in systemic risk for businesses using their services'.

machines as it enables the back up of data centrally and easily. The loss or malfunction of an employee's machine need not be a catastrophe for the employer since "the shift away from devices and into the cloud brings with it a shift in reliance on one's own ability to keep things safe to the ability of companies and organisations as trustees".[6] It is this structural aspect of the cloud that is however poorly understood by many. Rather than being anything as ethereal as a single cloud in the sky, cloud services are run along business lines, hosted on machines in a server storage network, run by the service provider and these businesses can fail.[7] In public clouds, the service provider's network of servers provides the cloud, and the failure of such a service provider will potentially heavily impact on users. Greater security is provided by private clouds, hosted on machines owned and controlled by the customer but these are notably more expensive than public clouds and, if third-party hosted, private clouds also present risks. Cloud-dependent activities would be undermined in the event of an insolvency of a public cloud service provider, or third party provider of private cloud services, potentially catastrophically, yet the implications of insolvencies in the digital economy sector, such as the prospect of a 'too big to fail' scenario, are only starting to be discussed.[8]

The potential for a problem of disruption to businesses using cloud computing services has so far only been legislatively recognised in one way. This recognition is from the perspective of the debtor, since technology suppliers are designated as essential suppliers.[9] This designation is required given the devastating impact that a loss of services can have on a struggling company. Looking at this same issue from a different perspective, the loss of IT services following the failure of a supplier would have impacts on a far greater range of users yet it is not similarly addressed, perhaps because of the practical difficulties that a requirement to keep IT companies trading would present. An example of a law that protects the interests of *users* is Art 567 of the Luxembourg Code de Commerce. As originally enacted this law enabled the recovery of goods entrusted to debtors upon the debtor's insolvency and in 2012 it was extended to include intangibles in recognition of the growing importance of cloud computing.[10] As will be considered in more detail later, having an entitlement to recover data in the event of the insolvency of a cloud service provider is only one problem since there must be temporary continuity of service to enable recovery to take place and this presents more difficult issues.

It is easy to see the potential economic harm that can be caused by a cloud computing insolvency. Anyone who has experienced even a temporary outage of online services will know the disruption this can have on productivity.[11] Disruption to cloud service provision could deny to the user access to data, software, platform and/or infrastructure, depending on the services used, and on an ongoing basis. Given the potentially significant impact of an insolvency in this sector it is important for there to be dialogue between the technology sector

---

[6] Patrick Ryan and Sarah Falvey, 'Trust in the Clouds' (2012) 28 *Computer Law & Security Review* 513.

[7] A US provider, Nirvanix, filed for US Chapter 11 bankruptcy protection in 2013 and gave customers two weeks' notice before closing down. Even such a small time window may not be available in all future cases. Other cloud providers which have gone out of business are Megaupload and MegaCloud, and the UK example of 2e2 is briefly discussed in this paper.

[8] J. Brodkin, 'Gartner: Seven Cloud-Computing Security Risks' (*InfoWorld,* 2008) <www.infoworld.com/d/securitycentral/gartner-seven-cloud-computing-security-risks853> 3 July 2008.

[9] Under IA 1986, s 233(3)(f) and 233A.

[10] Chambre de Commerce, 'Projet de loi portant modification de l'article 567 du Code de commerce' (4037SBE) <http://www.cc.lu/uploads/tx_userccavis/4037SBE_PL_art_567_Code_commerce_Avis_commun.pdf>. See also EuroCloud Luxembourg, 'Cloud Computing in Europe: Opportunities and Challenges' (February 2012).

[11] On the economic cost see e.g. Instor 'The Real Cost of Unplanned Downtime in 2019' <instor.com/blog/the-real-cost-of-unplanned-downtime-in-2019/> accessed 3 September 2020.

and the insolvency sector to identify problems, of which cloud computing insolvencies may only be one example, as well as proactive and reactive solutions but also important for attention to be paid at international level. Indeed what is notable about this growing significance of technology in ways of working is that technologies such as cloud computing are supranational technologies that are also complex and this prompts deeper reflection on the ability of domestic insolvency procedures to suffice since insolvencies in this sector are likely to be difficult to resolve and they may raise jurisdictional uncertainties.[12] The development of an international framework, would be desirable, but is likely to take time and in the interim domestic insolvency procedures can be analysed for suitability to handle technology cases and this will be the focus of this paper. England and Wales will be the jurisdictional focus and there will be an evaluation of the reforms that were made under the Corporate Insolvency and Governance Act 2020 as part of the response to the pandemic to assess how the augmented range of insolvency procedures may limit the impact of a cloud computing insolvency, which is arguably vital given new ways of working.

Complexities presented

Some brief points must first be made, however, regarding the potential complexities of insolvencies in the cloud computing sector that should illustrate why an insolvency in this sector could potentially be so disruptive in the light of new ways of working. The problem for the customer presented by a disruption to cloud services will be a loss of what the service provides, which could be infrastructure, platform and/or software.[13] For customers this could lead to problems including loss of access to data and potentially the means to process it, even the loss of this data in readable format altogether. Backups can partially address this problem but it is difficult to backup continuously so that backups will tend to be snapshots of data at a particular time. There are also problems of access as potentially large volumes of data will take time to withdraw and cloud computing arrangements can be structurally complex so that it can be difficult to locate data. The customer will face the disruption of downtime and the difficulties of finding replacement providers. It will not necessarily be the case that a replacement service can be found, for example, specialist software formerly accessed through the cloud may not be easily replaceable.

It should be added that it is presently difficult for customers to prepare for cloud computing insolvencies. It is notable that insolvency is barely addressed in the standard terms of cloud service providers.[14] In addition, many companies will find it difficult to negotiate an adjustment to the standard terms of clouds service providers to include detailed provision for insolvency, nor do standard terms typically provide any coverage of this matter. More powerful users may be able to include provision in their service level agreements, for example requiring notification if the service provider's financial position deteriorates and for protective steps to be taken to safeguard data. However, if the service provider fails to comply with these terms the user may be left only with a personal claim, which may well be worthless in a subsequent insolvency. Moreover, there are limitations to the extent to which

[12] One trend however is an increasing supranational reach of domestic laws of some states: Gideon Rachman, 'Beware the long arms of American and Chinese law' *Financial Times* 21 September 2020.

[13] The commonly used acronyms are SAAS, PAAS and IAAS, representing software as a service, platform as a service and infrastructure as a service.

[14] Johan David Michels, Christopher Millard and Felicity Turton, 'Contracts for Clouds, Revisited: An Analysis of the Standard Contracts for 40 Cloud Computing Services' (June 11, 2020). Queen Mary School of Law Legal Studies Research Paper No. 334/2020, Available at SSRN: <ssrn.com/abstract=3624712>

contractual entitlements, which include step-in rights,[15] software escrow[16] and copyright splitting,[17] can provide workable approaches in the event of a cloud service provider insolvency. There are also limitations to the extent that proprietary entitlements will help. It has already been noted that recovery of content from the cloud will not be straightforward.

Insolvency procedures

The options in the event of a cloud service provider suffering financial difficulties will be to reorganise the cloud service provider, with a view to ongoing trading, or to execute what we can term a 'managed closedown' offering temporary continuation of service in order that replacement services can be identified and content stored on the cloud can be extricated. A managed closedown would respond to demands to keep the service running temporarily to preserve and recover data and enable alterative provisions to be sourced. However, this would entail expense. Accordingly, a tension potentially arises between customers, who will want the service to keep running while they recover their data and make alterative arrangements, and creditors, who will not want further company resources to be depleted by ongoing trading and may favour immediate liquidation. It is likely that this will prove expensive for customers. For example, the administrator of the failed data centre operator 2e2 is reported to have requested funding from customers of almost £1 million to enable the business to continue operating and for customer data to be safeguarded and securely extracted, a process that was estimated to require 16 weeks of operation.[18]

To briefly recap on the reforms to the UK insolvency system, two new procedures, a moratorium[19] and a restructuring plan,[20] were inserted into existing Acts under the Corporate Insolvency and Governance Act 2002 to supplement the main existing collective restructuring options of administration, the CVA and the scheme of arrangement. Liquidation remains as the alterative offering a faster route for the closing down of the enterprise. Liquidation may be the favoured approach for creditors of the cloud enterprise as ongoing activities during a managed closedown will add costs without benefit for creditors. It is true that liquidation could feasibly be used for a managed closedown but the prospects of ongoing trading are limited as far as necessary towards beneficial winding up[21] and this does not logically entail continuation of service except where this will increase the sums available for creditors. Continued service is only likely to lead to additional costs.[22] It is these costs that present the greatest difficulties in this area, giving rise to a tension between the interests of creditors and those of cloud service customers. The insolvency procedures at present contain protections for creditors that can militate against the employment of rescue procedures in cloud service supplier cases.

---

[15] Common in outsourcing contracts. However, in the cloud computing context there would be difficulties presented where there is shared infrastructure, staff and technology.

[16] Where a third party holds software source code and releases it upon the occurrence of a triggering event, which could include the insolvency of the service provider.

[17] This would provide a potential solution to the problem of loss of means to read data, identified above, but it may be practicably difficult to implement in the event that there are numerous users of the software.

[18] '2e2 Datacentre Administrators Hold Customers' Data to £1m Ransom' (*ComputerWeekly.com* 8 February 2013) <https://www.computerweekly.com/news/2240177744/2e2-datacentre-administrators-hold-customers-data-to-1m-ransom>.

[19] IA 1986, Part A1.

[20] Companies Act 2006, Part 26A.

[21] IA 1986, Sch 4, para 5.

[22] See the 2e2 case discussed above.

The main pre-CIGA vehicle for providing protection to enable a managed close down of the business of a cloud service provider is administration and this is still potentially a good option for larger cloud service providers. Administration brings with it the protection of a moratorium which can enable the affairs of a company to be brought to an end without disruption from the claims of creditors. Questions arise, however, as to the compatibility of a managed close down with the availability of administration, where an appointment must be reasonably likely to achieve the purpose of administration.[23] The primary purpose of administration is to save the company[24] but if this is not reasonably practicable efforts can be focused on achieving a better return for creditors than would be likely if it was closed down without first going into administration,[25] or if that is not reasonably practicable to make a distribution to one or more secured or preferential creditors.[26] Since the managed close down of a cloud service provider would be likely to add costs without benefit to creditors it is this latter objective that would need to be relied on but there is a difficulty that the administrator must 'perform his functions in the interests of the company's creditors as a whole'.[27] It is also notable that administration may entail greater costs than debtor in possession proceedings. That is because if an administration appointment is made the moratorium protection comes at the cost of appointment of an administrator, although such an appointment brings expertise and can provide direction for a struggling business. An insolvency practitioner who takes control of a cloud service provider is likely to face a steep learning curve as well as many demands from customers and it is notable that a business of this nature will typically operate with a lean staffing level. One solution to enable the existing management, who will be familiar with the technicalities of a cloud service business, to remain in control under the protection of a moratorium could be the light touch administration protocol developed by the insolvency profession, under which a company in administration can be left under the control of its directors.[28] This model can potentially provide a suitable means for a managed closedown of a cloud service provider, however it should be added that such a delegation presents risks for the administrator and is only likely to be agreed to in an instance where the cloud service provider has sound and competent management to whom the administrator can delegate.

Given the potential difficulties of administration, the new restructuring moratorium might have been of benefit. In a new Insolvency Act 1986, Part A1 an eligible company is able to enjoy the benefit of a moratorium while under the supervision of a monitor. This procedure offers to company directors an alternative to the appointment of an administrator, which was the main previous way in which companies previously could have obtained the protection of a moratorium. This procedure can potentially avoid the costs of administration however the protection offered will be relatively brief, lasting for an initial 20 business days, although this period can be extended. Under the process for obtaining a moratorium where the cloud service provider is not subject to a winding up petition the directors are required to file inter alia a statement that the company is insolvent or approaching insolvency and a statement from a proposed monitor that the company has likely prospects of being rescued as a going concern.[29] It is this latter requirement that would prevent this route being used for a managed

[23] IA 1986, Sch B1, para 11, 18(3)(b) and 29(3)(b).
[24] IA 1986, Sch B1, para 3(1)(a).
[25] IA 1986, Sch B1, para 3(1)(b).
[26] IA 1986, Sch B1, para 3(1)(c).
[27] IA 1985, Sch B1, para 3(2).
[28] See R3, 'Light Touch Administration, A New Protocol' <https://www.r3.org.uk/press-policy-and-research/r3-blog/more/29357/page/1/light-touch-administration-a-new-protocol/>, 9 April 2020.
[29] IA 1986, s A6(1)(e).

closedown of a cloud service provider.[30] A cloud service provider which is subject to a winding up petition will only be able to obtain a moratorium following an order from the court in circumstances where this will provide a better result for the company's creditors as a whole than would be possible if the company were to be wound up without an initial period of moratorium protection.[31] Since a managed closedown primarily is required for the benefit of customers it may be difficult to argue that it would be for the benefit of creditors as a whole. Although the moratorium is therefore unsuitable for a managed close down in either situation it would potentially valuable in cases where the service provider is viable and ongoing trading is intended, since the moratorium could enable the company to enjoy temporary protection to enable reorganisation.

Of the other restructuring options, the new restructuring plan does not seem to offer an improved avenue for a managed closedown of a cloud service provider but might be useful in a case where the service provider has underlying ongoing viability.[32] Under a new Part 26A of the Companies Act 2006 a company can propose a restructuring plan. A plan will require approval by creditors, voting in classes, and/or by shareholders as well as by the court. A strong feature of the plan is that it introduces a possibility of a cross-class cramdown, enabling the court to approve a plan in circumstances where some classes have voted against it. However the requirement of two court hearings will mean that this option is only suitable for high value cases. A cheaper option would be the company voluntary arrangement but a company may need the additional protection of a moratorium during the agreement process. Protection may be needed to prevent a 'run on the banks' scenario in the event of damage to the reputation of the cloud service provider, causing customers to demand the recovery of their content from the cloud.[33]

Conclusion

This relatively brief article has focused on one sector of technology, cloud computing, and one jurisdiction, England and Wales. It is only possible to scratch the surface of this globally significant topic and there is much work to be done in identifying if there are any other complex areas of supranational technology that will have potential for significant impact of insolvencies. It is doubtful that domestic insolvency procedures will ever be adequate to address failures in this sector. There is a need for discussion at a global level of how insolvencies be addressed, and how improvements can be made to the infrastructure to support this. Given the breath of technologies this article has focused on cloud computing as there is here a clearly identified risk of insolvency having a significant impact. This is something that can potentially be exploited by a jurisdiction that can provide security of data and continuity of service in the event of insolvency as it can attract cloud service providers which can then offer confidence to customers. A special procedure for cloud service providers, enabling a managed close down, would be one possibility. In the longer term the development of robust laws to handle cloud computing insolvencies requires collaboration between data scientists and insolvency lawyers and attention on a global scale.

[30] There are other eligibility requirements in IA 1986, s A2 and Sch ZA1.
[31] IA 1986, s A4(5).
[32] See for example the Chapter 11 restructuring of Fusion Connect Inc.
[33] European Network and Information Security Agency, 'Cloud Computing, Benefits, Risks and Recommendations for Information Security' (December 2012), 19.